

**RECEIVED
CENTRAL FAX CENTER**

APR 29 2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Applicant: Morgan)	Art Unit: 2132
)	
Serial No.: 09/872,797)	Examiner: Dinh
)	
Filed: June 1, 2001)	ARC920000133US1
)	
For: INTERNET AUTHENTICATION WITH MULTIPLE)	April 29, 2005
INDEPENDENT CERTIFICATE AUTHORITIES)	750 B STREET, Suite 3120
)	San Diego, CA 92101
)	

APPEAL BRIEF

Commissioner of Patents and Trademarks

Dear Sir:

This brief is submitted under 35 U.S.C. §134 and is in accordance with 37 C.F.R. Parts 1, 5, 10, 11, and 41, effective September 13, 2004 and published at 69 Fed. Reg. 155 (August 2004). This brief is further to Appellant's Notice of Appeal filed herewith.

Table of Contents

<u>Section</u>	<u>Title</u>	<u>Page</u>
(1)	Real Party in Interest.....	2
(2)	Related Appeals/Interferences.....	2
(3)	Status of Claims.....	2
(4)	Status of Amendments.....	2
(5)	Concise Explanation of Subject Matter in Each Independent Claim.	2
(6)	Grounds of Rejection to be Reviewed.....	3
(7)	Argument.....	4
App.A	Appealed Claims	
App.B	Evidence Appendix	
App.C	Related Proceedings Appendix	

1053-112.APP

05/03/2005 MBIZUNES 00000060 090441 09872797

01 FC:1402 500.00 DA

CASE NO.: ARC920000133US1**Serial No.: 09/872,797****April 29, 2005****Page 2****PATENT**
Filed: June 1, 2001**(1) Real Party in Interest**

The real party in interest is IBM Corp.

(2) Related Appeals/Interferences

No other appeals or interferences exist which relate to the present application or appeal.

(3) Status of Claims

Claims 1-18 are pending and finally rejected.

(4) Status of Amendments

No amendments are outstanding.

(5) Concise Explanation of Subject Matter in Each Independent Claim, with Page and Figure Nos.

As an initial matter, it is noted that according to the Patent Office, the concise explanations under this section are for Board convenience, and do not supersede what the claims actually state, 69 Fed. Reg. 155 (August 2004), see page 49976. Accordingly, nothing in this Section should be construed as an estoppel that limits the actual claim language.

Claim 1 recites a computer authentication protocol that requires sending a certificate payload from a transmitting computer to a receiving computer, figure 1, page 7. The certificate payload includes at least two certificates, with each being generated by a respective certificate authority (reference numerals 20, 24,

1053-112.APP

CASE NO.: ARC920000133US1
Serial No.: 09/872,797
April 29, 2005
Page 3

PATENT
Filed: June 1, 2001

figure 1, page 7, last paragraph) and with the certificate authorities being independent of each other such that no trust relationship exists between the CAs, id.

The references in the first paragraph of this section are incorporated herein. Claim 7 sets forth a computer program device that has a computer program storage device including a program of instructions usable by a computer, page 8, first three paragraphs and figure 1. Means are provided for combining a first entity identification (ID) with a second entity ID to render an ID payload, figure 3, page 9, first full paragraph. Also, means send the ID payload to a computer along with at least one certificate payload, id.

The references in the above paragraphs of this section are incorporated herein. Claim 10 sets forth a computer program device that has a computer program storage device including a program of instructions usable by a computer. Means are provided for generating a signature payload by concatenating at least two signatures of respective entities, and means send the signature payload to a computer along with at least one certificate payload.

The references in the above paragraphs of this section are incorporated herein. Claim 13 sets forth a computer system for secure network authentication that has at least one host certificate authority (CA) generating a host authentication certificate for at least one host computer, and at least one user CA generating a user authentication certificate for at least one user. The certificates can be combined into a certificate payload during an authentication process, and the host CA is not in a trust relationship with the user CA and vice-versa.

(6) Grounds of Rejection to be Reviewed on Appeal

Claims 1-18 have been rejected under 35 U.S.C. §103 as being unpatentable over Harkins et al. (RFC document) in view of Asay et al., USPN 5,903,882.

1053-112.APP

CASE NO.: ARC920000133US1
Serial No.: 09/872,797
April 29, 2005
Page 4

PATENT
Filed: June 1, 2001

(7) Argument

As an initial matter, it is noted that according to the Patent Office, a new ground of rejection in an examiner's answer should be "rare", and should be levied only in response to such things as newly presented arguments by Applicant or to address a claim that the examiner previously failed to address, 69 Fed. Reg. 155 (August 2004), see, e.g., pages 49963 and 49980. Furthermore, a new ground of rejection must be approved by the Technology Center Director or designee and in any case must come accompanied with the initials of the conferees of the appeal conference, *id.*, page 49979.

The issue is simple so Appellant will keep things short. The rejection admits that the primary reference fails to teach two certificates generated by respective CAs that are independent of each other, but alleges that Asay et al. in various sections including col. 32, lines 9-19, col. 33, lines 14-19, col. 37, lines 25-60, figure 6, elements 206 and 208, and figure 8 supplies the missing teaching. This is incorrect. Col. 32, lines 9-17 make clear that a single certificate is used, although the source of the certificate could be one of several CAs or sponsors. In other words, Asay et al. makes clear that one or the other certificate source is used but not both: "A subscriber is issued one or more certificates from a certification authority within a hierarchy of certification authorities 206 *OR* from one of a number of sponsors 208", col. 32, lines 11-14 (emphasis mine). Thus, no matter how many certificates are issued to a subscriber, they all come from either element 206 or from element 208 but not both as required in Claims 1 and 13. For this reason, the rejections should be reversed.

Additionally, it is not at all clear that the relied-upon certificate authorities 206 are not in trust relationships with the sponsors 208 as otherwise alleged in reliance on figure 6 and col. 32, lines 9-19. In fact, if anything the opposite appears to be true. Asay et al., col. 32, line 19 explicitly envisions that the

1053-112.APP

CASE NO.: ARC920000133US1
Serial No.: 09/872,797
April 29, 2005
Page 5

PATENT
Filed: June 1, 2001

certificate authorities 206 and sponsors 208 "may share directories". If Asay et al. permits shared directories in one implementation, this strongly suggests that a trust relationship is contemplated between the two. Moreover, col. 33, lines 45-50 clearly explain that the global liability tracking server 220 can be part of the CAs 206 or sponsors 208. If the system-wide liability tracking server is part of a CA 206, then the CA 206, to execute the intended system-wide liability tracking, seemingly must be in a trust relationship with a sponsor 208. Accordingly, to interpret Asay et al. that the certificate authorities 206 and sponsors 208 are not in a trust relationship with each other not only is obvious hindsight, since Asay et al. suggests the precise opposite, but it borders on the illogical.

With respect to independent Claim 7, the rejection readily admits that the primary reference fails to teach a second ID, much less combining it with a first ID in an ID payload that is sent to a computer along with a certificate payload, but alleges that the figure 8 of Asay et al. remedy this shortfall. The examiner appears to have relied on a false syllogism, essentially arriving at a conclusion that is not supported by the major and minor premises, namely, that because a message in figure 8 of Asay et al. carries a device certificate and a subscriber certificate, and per the examiner each certificate must have an ID, then it follows that two IDs must be in the payload. Not only does the conclusion not flow from the premises (it is logically possible to send something such as a certificate without sending its ID as well), it misunderstands what Claim 7 actually recites, which is combining a first entity identification (ID) with a second entity ID to render an ID payload, and sending the ID payload to a computer *along with* a certificate payload. That is, the IDs being combined in Claim 7 are those of entities; even if the certificates in Asay et al. have IDs, no suggestion appears to send them in an ID payload separate from the certificates, much less that the certificate IDs be transmogrified into entity IDs and then sent in an ID payload. So the examiner's point that multiple

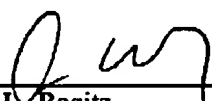
1053-112.APP

CASE NO.: ARC920000133US1
Serial No.: 09/872,797
April 29, 2005
Page 6

PATENT
Filed: June 1, 2001

certificate IDs are used in Asay et al. not only is logically unsupportable, it is irrelevant to what Claim 7 actually requires. Likewise, Claim 10 is patentable over Asay et al. because Claim 10 requires the concatenation of two entity signatures, as opposed to two certificate IDs, and then sending the concatenation along with a certificate payload.

Respectfully submitted,



John D. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1053-112.APP

CASE NO.: ARC920000133US1

Serial No.: 09/872,797

April 29, 2005

Page 7

PATENT
Filed: June 1, 2001**APPENDIX A - APPEALED CLAIMS**

1. A computer authentication protocol, comprising:
sending at least one certificate payload from a transmitting computer to a receiving computer, the certificate payload including at least two certificates each being generated by a respective certificate authority (CA), the certificate authorities being independent of each other such that no trust relationship exists between the CAs.
2. The protocol of claim 1, wherein the certificates are concatenated together.
3. The protocol of Claim 2, wherein at least one certificate is associated with a person and one certificate is associated with a host computer.
4. The protocol of Claim 1, further comprising sending at least one Identification (ID) payload between the computers, the ID payload being generated by combining the IDs of at least two entities.
5. The protocol of Claim 4, further comprising sending at least one signature payload between the computers, the signature payload being generated by concatenating the signatures of at least two entities.
6. The protocol of Claim 5, wherein each signature is formed by applying a pseudorandom function (PRF) to at least the associated ID to render a result, and then encrypting the result with a private key associated with the entity represented by the ID.
7. A computer program device, comprising:
a computer program storage device including a program of instructions usable by a computer, comprising:
logic means for combining a first entity identification (ID) with a second entity ID to render an ID payload; and
logic means for sending the ID payload to a computer along with at least one certificate payload.
8. The computer program device of Claim 7, further comprising:
logic means for generating a signature payload by concatenating at least two signatures of respective entities.
9. The computer program device of Claim 8, wherein the means for generating a signature payload applies a pseudorandom function (PRF) to at least an ID associated with an entity to render a result, and then encrypting the result with a private key associated with the entity represented by the respective ID.
10. A computer program device, comprising:
a computer program storage device including a program of instructions usable by a computer, comprising:

1053-112.APP

CASE NO.: ARC920000133US1

Serial No.: 09/872,797

April 29, 2005

Page 8

PATENT

Filed: June 1, 2001

logic means for generating a signature payload by concatenating at least two signatures of respective entities; and

logic means for sending the signature payload to a computer along with at least one certificate payload.

11. The computer program device of Claim 10, wherein the means for generating a signature payload applies a pseudorandom function (PRF) to at least an ID associated with an entity to render a result, and then encrypting the result with a private key associated with the entity represented by the respective ID.

12. The computer program device of Claim 11, further comprising:

logic means for combining a first entity ID with a second entity ID to render an ID payload;

and

logic means for sending the ID payload to a computer along with at least one certificate payload.

13. A computer system for secure network authentication, comprising:

at least one host certificate authority (CA) generating a host authentication certificate for at least one host computer; and

at least one user CA generating a user authentication certificate for at least one user, wherein the certificates can be combined into a certificate payload during an authentication process, the host CA not being in a trust relationship with the user CA and vice-versa.

14. The system of claim 13, wherein the certificates are concatenated together to establish a certificate payload.

15. The system of Claim 14, wherein at least one certificate is associated with a person and one certificate is associated with a host computer.

16. The system of Claim 13, wherein the system sends at least one identification (ID) payload between the computers, the ID payload being generated by combining the IDs of at least two entities.

17. The system of Claim 16, wherein the system sends at least one signature payload between the computers, the signature payload being generated by concatenating the signatures of at least two entities.

18. The system of Claim 17, wherein each signature is formed by applying a pseudorandom function (PRF) to at least the associated ID to render a result, and then encrypting the result with a private key associated with the entity represented by the ID.

1053-112.APP

CASE NO.: ARC920000133US1
Serial No.: 09/872,797
April 29, 2005
Page 9

PATENT
Filed: June 1, 2001

APPENDIX B - EVIDENCE

None (this sheet made necessary by 69 Fed. Reg. 155 (August 2004), page 49978.)

1053.112.APP

CASE NO.: ARC920000133US1
Serial No.: 09/872,797
April 29, 2005
Page 10

PATENT
Filed: June 1, 2001

APPENDIX C - RELATED PROCEEDINGS

None (this sheet made necessary by 69 Fed. Reg. 155 (August 2004), page 49978.)

1053-112.APP